



Network security

11/15/07

EJ Jung



Chapter 8: Network Security

Chapter goals:

- ◆ understand principles of network security:
 - cryptography and its *many* uses beyond "confidentiality"
 - authentication
 - message integrity
- ◆ security in practice:
 - firewalls and intrusion detection systems
 - security in application, transport, network, link layers



Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 End point authentication

8.5 Securing e-mail

8.6 Securing TCP connections: SSL

8.7 Network layer security: IPsec

8.8 Securing wireless LANs

8.9 Operational security: firewalls and IDS



What is network security?

Confidentiality: only sender, intended receiver should “understand” message contents

- sender encrypts message
- receiver decrypts message

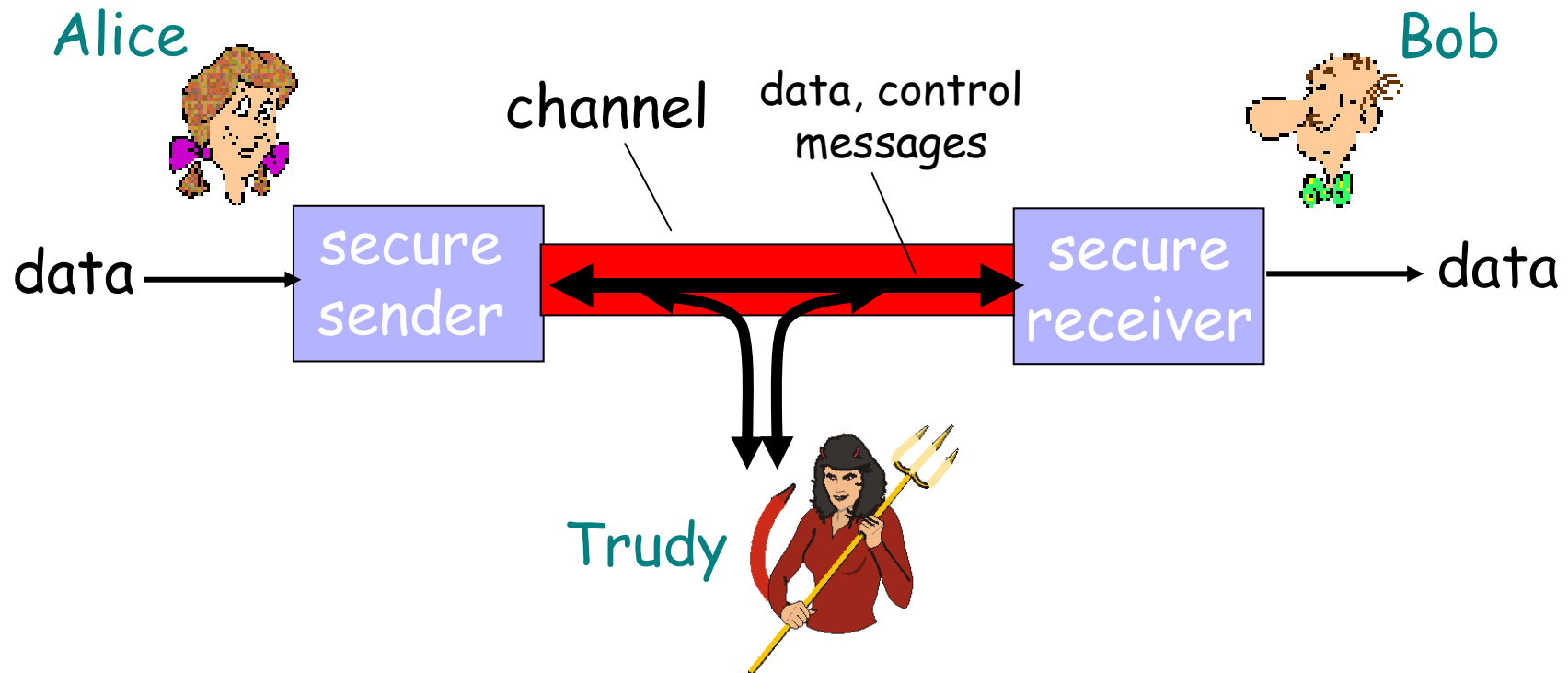
Authentication: sender, receiver want to confirm identity of each other

Message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Access and availability: services must be accessible and available to users

Friends and enemies: Alice, Bob, Trudy

- ◆ well-known in network security world
- ◆ Bob, Alice want to communicate “securely”
- ◆ Trudy (intruder) may intercept, delete, add messages





Who might Bob, Alice be?

- ◆ ... well, *real-life* Bobs and Alices!
- ◆ Web browser/server for electronic transactions (e.g., on-line purchases)
- ◆ on-line banking client/server
- ◆ DNS servers
- ◆ routers exchanging routing table updates
- ◆ other examples?



There are bad people out there!

Q: What can a "bad guy" do?

A: a lot!

- *eavesdrop*: intercept messages
- actively *insert* messages into connection
- *impersonation*: can fake (spoof) source address in packet (or any field in packet)
- *hijacking*: "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)

more on this later



Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 End point authentication

8.5 Securing e-mail

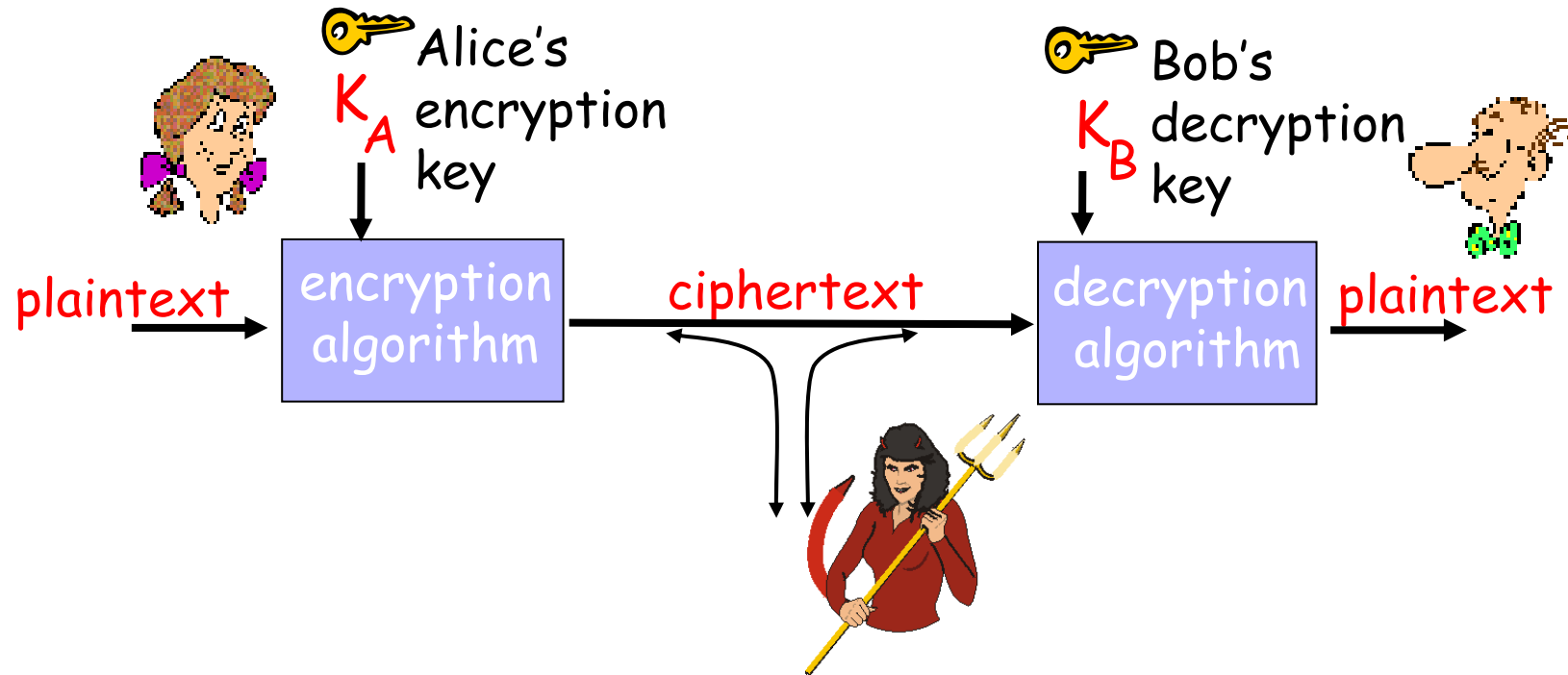
8.6 Securing TCP connections: SSL

8.7 Network layer security: IPsec

8.8 Securing wireless LANs

8.9 Operational security: firewalls and IDS

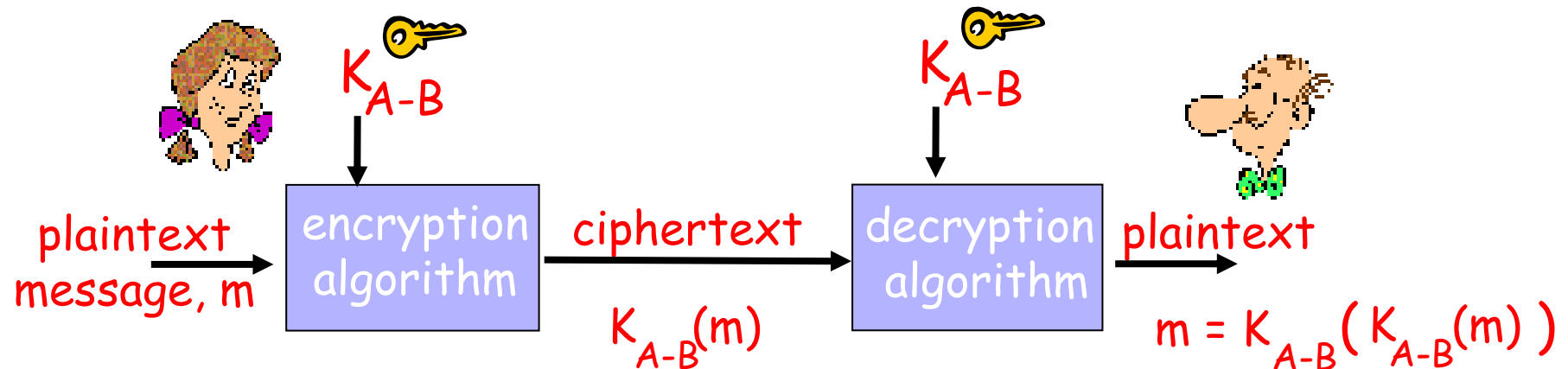
The language of cryptography



symmetric key crypto: sender, receiver keys *identical*

public-key crypto: encryption key *public*, decryption key *secret* (private)

Symmetric key cryptography



symmetric key crypto: Bob and Alice share know same (symmetric) key: K_{A-B}

- ◆ e.g., key is knowing substitution pattern in mono alphabetic substitution cipher
- ◆ Q: how do Bob and Alice agree on key value?



Symmetric key crypto: DES

DES: Data Encryption Standard

- ◆ US encryption standard [NIST 1993]
- ◆ 56-bit symmetric key, 64-bit plaintext input
- ◆ How secure is DES?
 - DES Challenge: 56-bit-key-encrypted phrase (“Strong cryptography makes the world a safer place”) decrypted (brute force) in 4 months
 - no known “backdoor” decryption approach
- ◆ making DES more secure:
 - use three keys sequentially (3-DES) on each datum
 - use cipher-block chaining



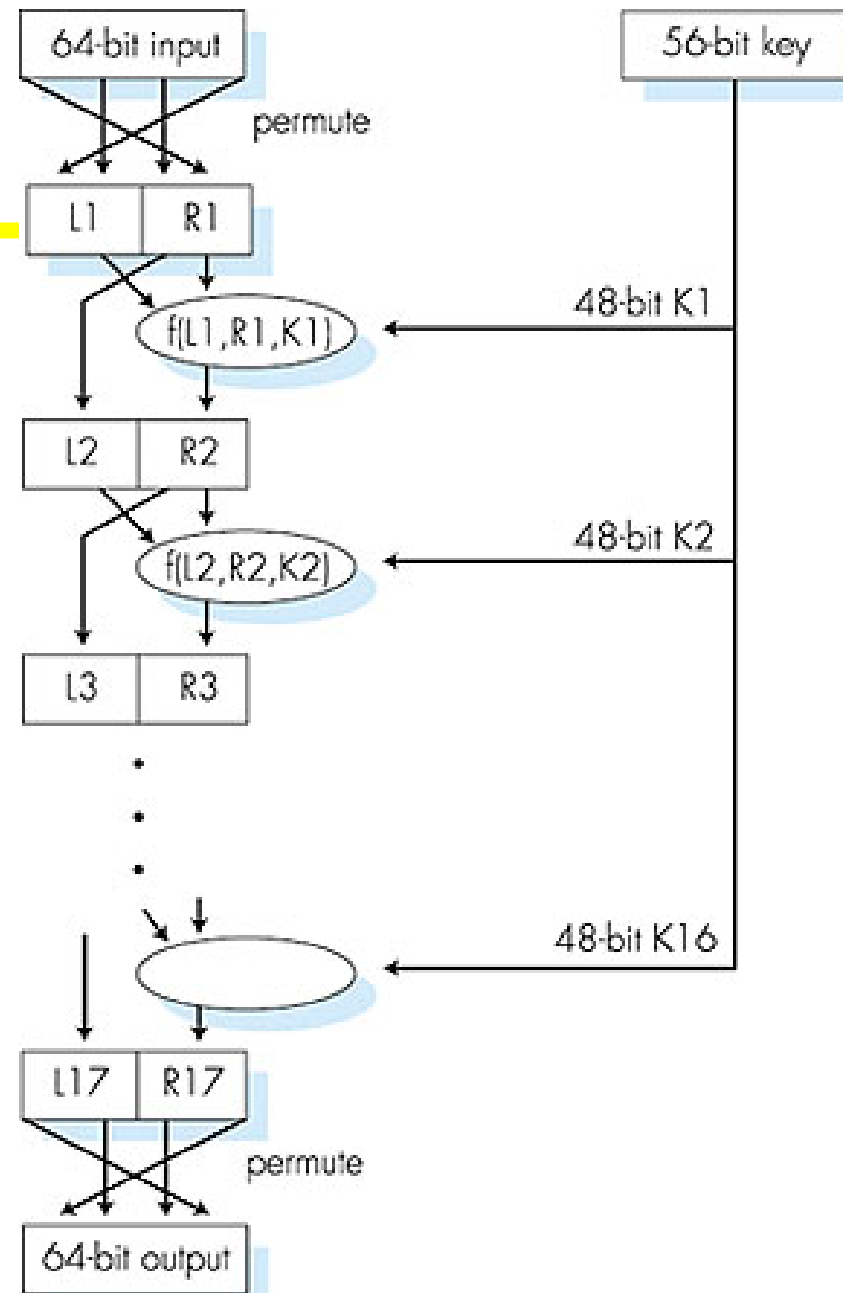
Symmetric key crypto: DES

DES operation

initial permutation

16 identical "rounds" of
function application,
each using different 48
bits of key

final permutation





AES: Advanced Encryption Standard

- ◆ new (Nov. 2001) symmetric-key NIST standard, replacing DES
- ◆ processes data in 128 bit blocks
- ◆ 128, 192, or 256 bit keys
- ◆ brute force decryption (try each key) taking 1 sec on DES, takes 149 trillion years for AES